BEZPEČNOSTNÍ AUDIT

Tento dokument představuje anonymizované výsledky bezpečnostního auditu pomocí řešení Safetica. Analýza byla provedena na 83 stanicích v období od 1. 3. 2019 do 19. 3. 2019. Výsledky se týkají pouze běžné pracovní doby (od 07:00 do 16:00 hodin).

safetica®

Obsah

ROZSAH AUDITU

Bezpečnostní audit se zaměřuje na citlivá data v prostředí společnosti, na soubory, které opouštějí společnost a na aktivitivy zaměstnanců s prostředky společnosti.

Audit vychází z monitorovaných dat a aktivit uživatelů na stanicích, kde bylo nasazeno řešení Safetica. Bezpečnostní problémy a doporučená opatření vychází z toho, jak bylo v Safetica nastaveno, co je citlivý obsah společnosti, jaké jsou bezpečné způsoby pro přenos citlivého obsahu a jaké jsou rizikové aktivity zaměstnanců.

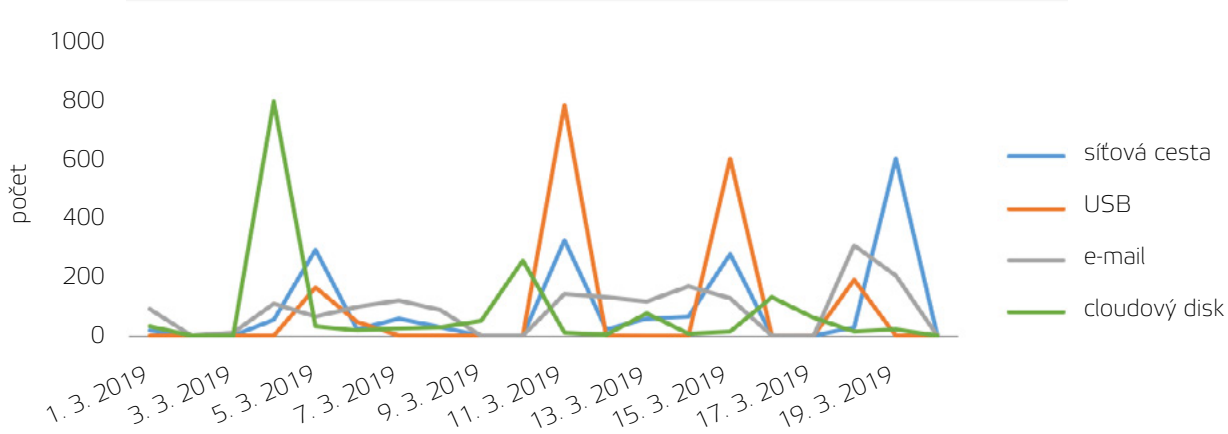
Monitorovaná data:

- **301 GB** dat
- **91.599** operací se soubory
- **33.032** souborů
- **4.240** odchozích souborů

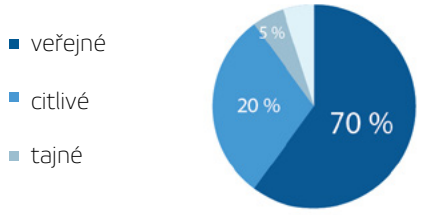
Monitorované prostředí:

- **321** uživatelských účtů
- **83** počítačů se Safeticou
- **223** počítačů celkově
- **42** administrátorů Safetica

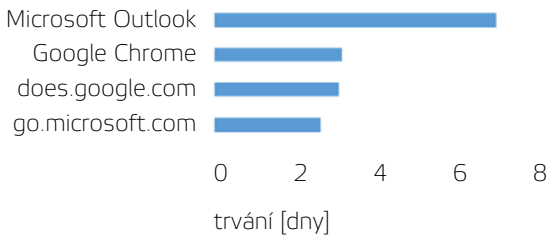
Kdy soubory odešly?



Jaké datové kategorie měly soubory?



Co byly nejčastější činnosti?



V případě bezpečnostních incidentů budete varováni okamžitými upozorněními.

Pokud nastane bezpečnostní incident, tak je rychlá reakce důležitá kvůli minimalizaci negativních dopadů. Okamžité varování zodpovědným osobám pomůže rychle pochopit, kde nastal problém.

Máte nastaveny pravidelné zprávy o bezpečnostním stavu společnosti.

Pravidelná kontrola bezpečnostního stavu společnosti je nepostradatelnou součástí celkové bezpečnostní strategie.

Identifikovali jste, která data jsou citlivá a je potřeba je chránit.

Bez znalosti toho, co jsou citlivá data společnosti, není možné vytvořit bezpečnostní politiky a zabránit tak únikům dat.

Doporučení:

- Nastavte okamžitá e-mailová varování pro všechny bezpečnostní incidenty, které chcete sledovat.
- Kontrolujte, že nastavená okamžitá varování jsou aktuální a jsou adresována zodpovědným osobám.
- Nastavte automatizované reporty na všechny relevantní oblasti.
- Kontrolujte, že reporty jsou aktuální a jsou adresovány zodpovědným osobám.
- Kontrolujte soubory, se kterými zaměstnanci pracují, a identifikujte citlivá data.
- Kategorizujte citlivé soubory do datových kategorií.

SOUBORY ODCHÁZEJÍCÍ PŘES USB A JINÁ EXTERNÍ ZAŘÍZENÍ

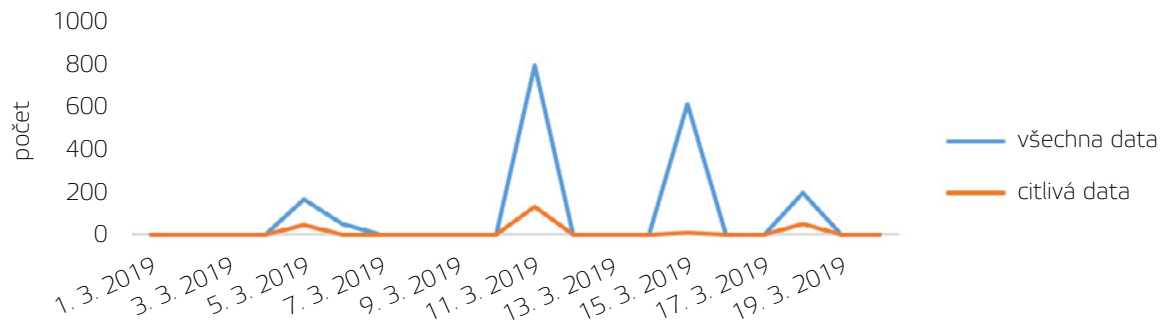
Nahrání velkého objemu citlivých dat na USB flash disk je velmi snadný a rychlý způsob, jak může společnost přijít o kontrolu nad svými daty. Následná ztráta či krádež USB flash disku pak vede k tomu, že se kritická data dostanou do nepovolaných rukou.

⚠ 223 citlivých souborů z celkem 1793 souborů bylo odesláno prostřednictvím kanálu USB a jiná externí zařízení. Vaše bezpečnostní politiky nebyly v režimu blokování.

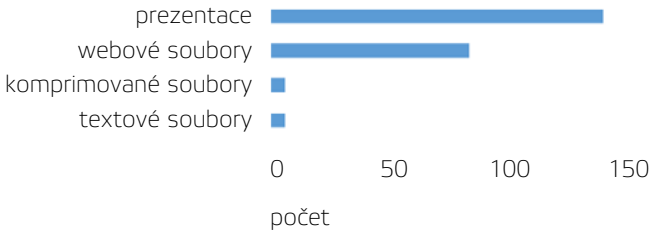
Vynesení dat mimo společnost pomocí USB zařízení představuje významné riziko. Určení zabezpečených USB zařízení, která jsou povolená, je základní předpoklad bezpečnostních opatření.

✓ 15 citlivých souborů z celkem 16 souborů bylo odesláno prostřednictvím kanálu USB a jiná externí zařízení se řídily vašimi bezpečnostními politikami.

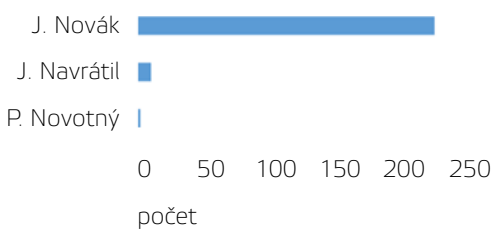
Kdy soubory odešly?



Které kategorie citlivých souborů odešly?



Kdo odeslal nejvíce citlivých souborů?



ℹ **Doporučení:**

- Určete a kontrolujte, která USB a jiná externí zařízení jsou důvěryhodná.
- Vyhodnocujte, jaké soubory odchází. Prověřujte, jestli by neměly být kategorizovány jako citlivé.
- USB a jiná externí zařízení, která nejsou důvěryhodná, omezte pouze pro čtení nebo je zakažte úplně.
- Nastavte DLP politiky pro přenos citlivých souborů na USB a jiná externí zařízení.
- Nastavte upozornění, pokud citlivé soubory odchází na nedůvěryhodná USB.
- Nastavte e-mailová varování, když někdo kopíruje velké množství souborů na USB.

SOUBORY ODCHÁZEJÍCÍ E-MAILEM

Odeslání e-mailu s přílohou je jeden z nejsnadnějších způsobů, jak dochází k úniku citlivých dat. Ve většině případů se přitom nejedná o úmyslné poškození společnosti, ale o pouhý omyl – vložení špatného příjemce nebo nesprávné přílohy.

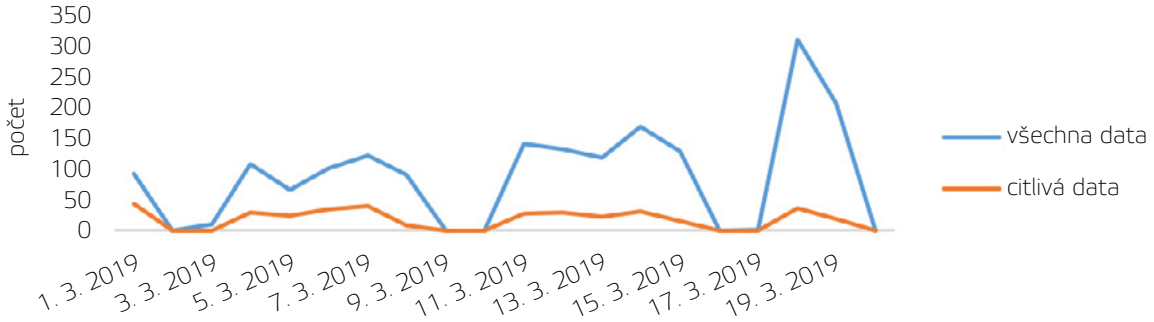
5 citlivých souborů z celkem 136 souborů bylo odesláno prostřednictvím kanálu e-maily. Tyto soubory nebyly řízeny žádnou bezpečnostní politikou.

E-maily s citlivými daty by měly jít pouze důvěryhodným příjemcům, kteří s daty potřebují pracovat.

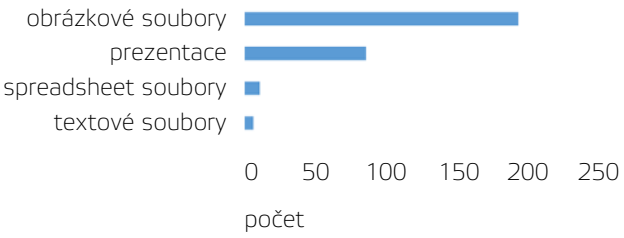
124 citlivých souborů z celkem 124 souborů bylo odesláno prostřednictvím kanálu e-maily. Vaše bezpečnostní politiky nebyly v režimu blokování.

241 citlivých souborů z celkem 1586 souborů bylo odesláno prostřednictvím kanálu e-maily. Tyto soubory se řídily vašimi bezpečnostními politikami.

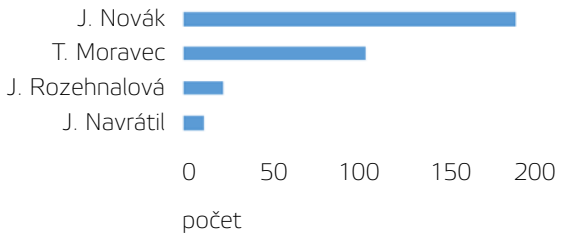
Kdy soubory odešly?



Které kategorie citlivých souborů odešly?



Kdo odeslal nejvíce citlivých souborů?



Doporučení:

- Určete a kontrolujte, jaké jsou důvěryhodné e-mailové domény společnosti.
- Vyhodnocujte, jaké přílohy odchází v e-mailech. Prověřujte, jestli by e-mailové přílohy neměly být kategorizovány jako citlivé soubory.
- Nastavte DLP politiky pro posílání citlivých souborů prostřednictvím e-mailu.
- Nastavte okamžité e-mailové varování, pokud citlivé soubory odchází na nedůvěryhodné e-mailové domény.

SOUBORY ODCHÁZEJÍCÍ WEBMAILEM

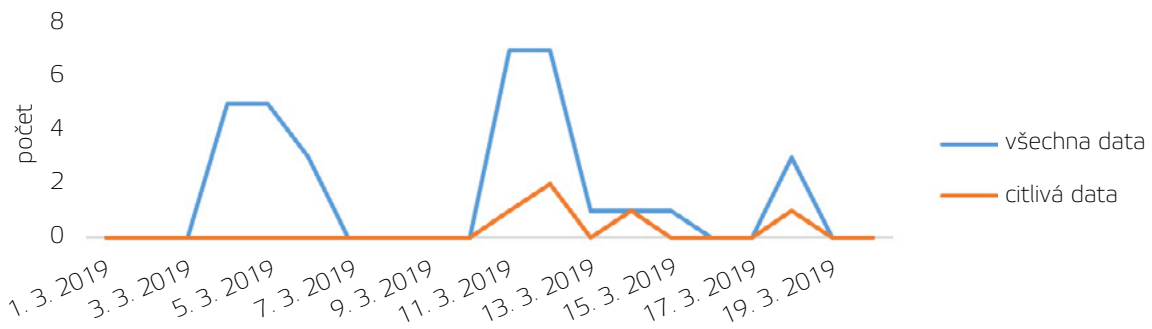
Webové e-mailové služby jsou populární způsob, jak komunikovat i posílat citlivá data. Současně s tím ale vzrůstá riziko dalšího kanálu, který je potřeba ošetřit před potenciálním únikem dat.

3 citlivých souborů z celkem 31 souborů bylo odesláno prostřednictvím kanálu webmaily. Vaše bezpečnostní politiky nebyly v režimu blokování.

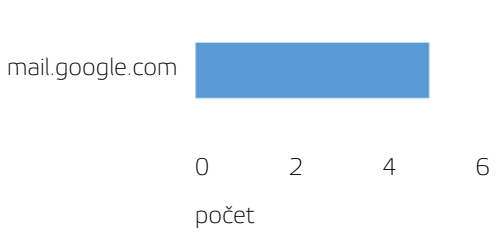
Používání webových e-mailových služeb pro rozesílání citlivého obsahu je bezpečnostní problém, protože nelze na koncové stanici zabezpečit, jaká data a komu jsou posílána.

2 citlivých souborů z celkem 2 souborů bylo odesláno prostřednictvím kanálu webmaily. Tyto soubory se řídily vašimi bezpečnostními politikami.

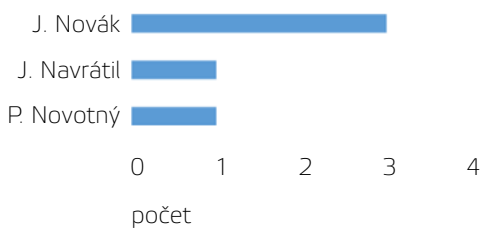
Kdy soubory odešly?



Kam citlivé soubory odešly?



Kdo odeslal nejvíce citlivých souborů?



Doporučení:

- Určete a kontrolujte, jaké jsou důvěryhodné webmailové domény společnosti.
- Vyhodnocujte, jaké soubory jsou odesílány. Prověřujte, jestli by neměly být kategorizovány jako citlivé.
- Nastavte DLP politiky pro posílání citlivých souborů prostřednictvím webmailu.
- Nastavte upozornění, pokud citlivé soubory odchází na nedůvěryhodné webmailové domény.

SOUBORY NAHRANÉ NA WEB

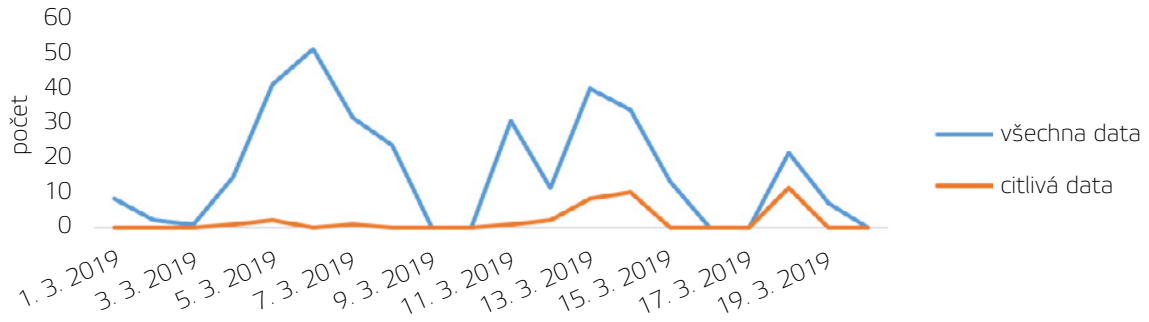
Nahrání souborů na web je oblíbený způsob, kterým zaměstnanci mohou sdílet například větší soubory, které nejdou poslat jako příloha e-mailu. Je proto důležité určit pravidla pro posílání souborů tímto kanálem.

11 citlivých souborů z celkem 301 souborů bylo odesláno prostřednictvím kanálu nahrání na web. Vaše bezpečnostní politiky nebyly v režimu blokování.

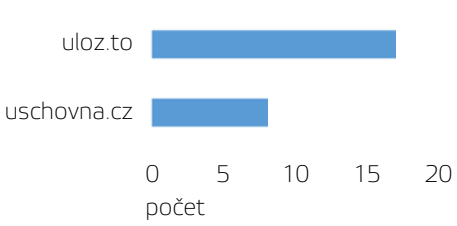
Soubory společnosti, které jsou nahrány na veřejné weby, mohou být okamžitě staženy cizí osobou a ztrácíte tak nad nimi kontrolu.

25 citlivých souborů z celkem 25 souborů bylo odesláno prostřednictvím kanálu nahrání na web. Tyto soubory se řídily vašimi bezpečnostními politikami.

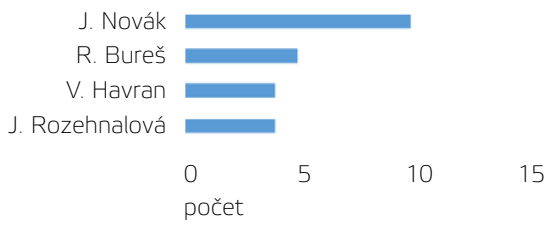
Kdy soubory odešly?



Kam citlivé soubory odešly?



Kdo odeslal nejvíce citlivých souborů?



Doporučení:

- Určete a kontrolujte, jaké jsou důvěryhodné webové stránky společnosti.
- Vyhodnocujte, jaké soubory jsou odesílány. Prověřujte, jestli by neměly být kategorizovány jako citlivé.
- Nastavte DLP politiky pro nahrávání citlivých souborů na webové stránky.
- Nastavte upozornění, pokud citlivé soubory odchází na nedůvěryhodné webové stránky.

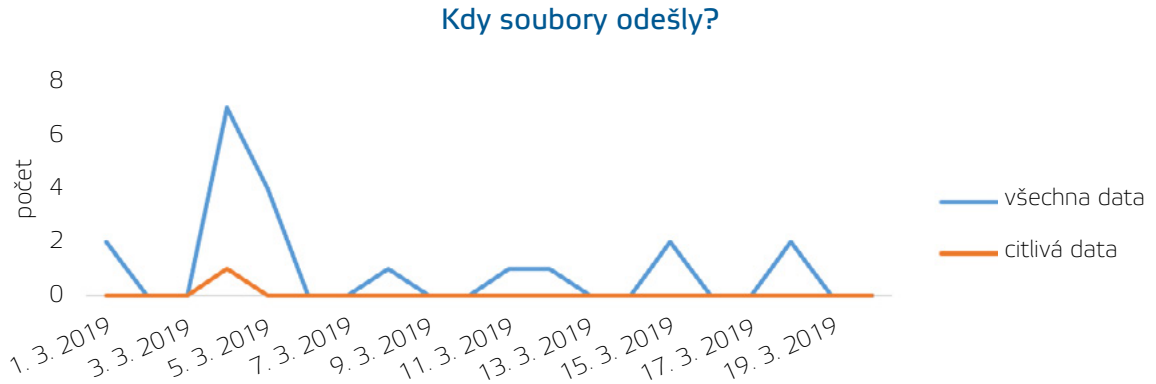
SOUBORY ODCHÁZEJÍCÍ APLIKACEMI PRO INSTANT MESSAGING

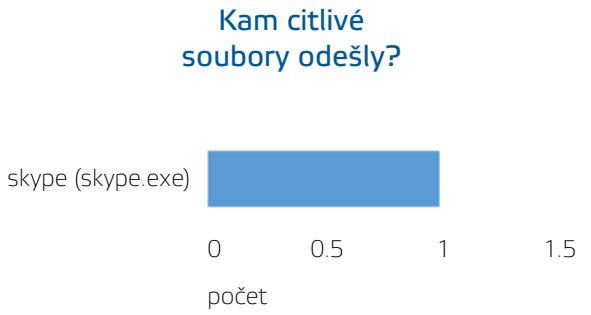
Aplikace pro instant messaging jsou komunikačním nástrojem pro spolupráci s kolegy i partnery po celém světě. I když je posílání souborů omezeno na malý okruh příjemců, představuje instant messaging hrozbu pro společnosti, které nekontrolují a neřídí použití těchto aplikací.

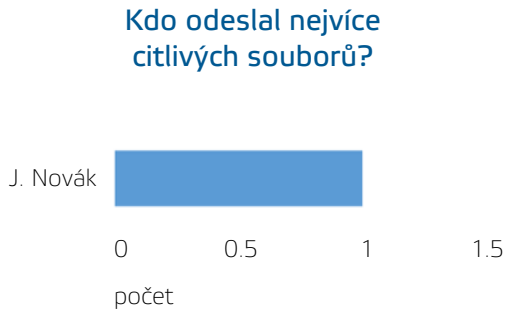
⚠ 18 souborů bylo odesláno prostřednictvím kanálu instant messaging. Vaše bezpečnostní politiky nebyly v režimu blokování.

Nekontrolované posílání souborů společnosti prostřednictvím instant messaging aplikací ohrožuje bezpečnost dat.

✓ 1 citlivých souborů z celkem 2 souborů bylo odesláno prostřednictvím kanálu instant messaging. Tyto soubory se řídily vašimi bezpečnostními politikami.







Doporučení:

- Vyhodnocujte, jaké soubory jsou odesílány. Prověřujte, jestli by neměly být kategorizovány jako citlivé.
- Nastavte DLP politiky pro posílání citlivých souborů prostřednictvím aplikací pro instant messaging.

SOUBORY ODCHÁZEJÍCÍ PŘES CLOUDOVÉ ÚLOŽIŠTĚ

Únik souborů společnosti může nastat například tehdy, když jsou data nahrána na soukromá cloudová úložiště a kvůli špatnému nastavení jsou přístupná třetím osobám.

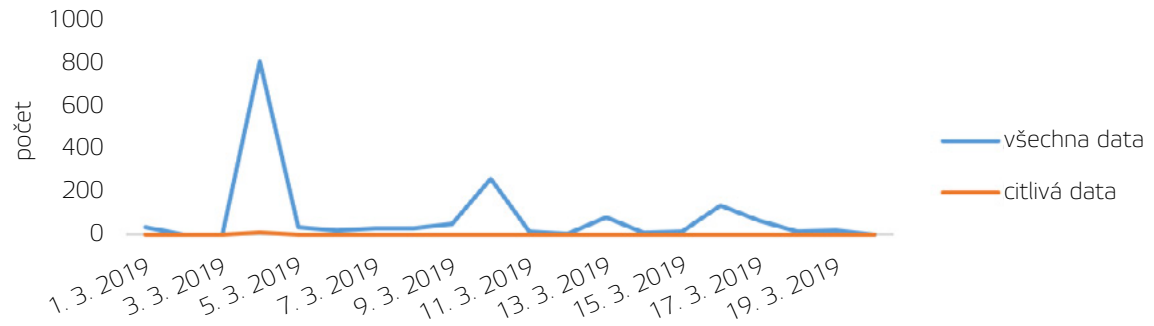
⚠ 21 souborů bylo odesláno prostřednictvím kanálu cloudová úložiště. Tyto soubory nebyly řízeny žádnou bezpečnostní politikou.

Používání soukromých cloudových úložišť a nepovolených cloudových úložišť představuje riziko pro citlivá data společnosti.

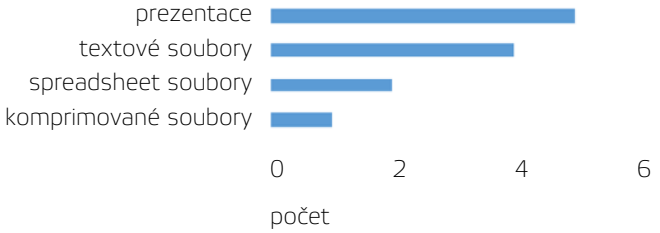
⚠ 10 citlivých souborů z celkem 678 souborů bylo odesláno prostřednictvím kanálu cloudová úložiště. Vaše bezpečnostní politiky nebyly v režimu blokování.

✓ 2 citlivých souborů z celkem 929 souborů bylo odesláno prostřednictvím kanálu cloudová úložiště. Tyto soubory se řídily vašimi bezpečnostními politikami.

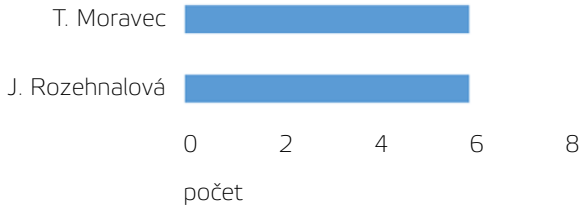
Kdy soubory odešly?



Které kategorie citlivých souborů odešly?



Kdo odeslal nejvíce citlivých souborů?



Doporučení:

- Vyhodnocujte, jaké soubory jsou odesílány. Prověřujte, jestli by neměly být kategorizovány jako citlivé.
- Nastavte DLP politiky pro posílání citlivých souborů prostřednictvím cloudových úložišť.
- Zamezte použití cloudových úložišť, která nejsou nezbytná pro vaši společnost.

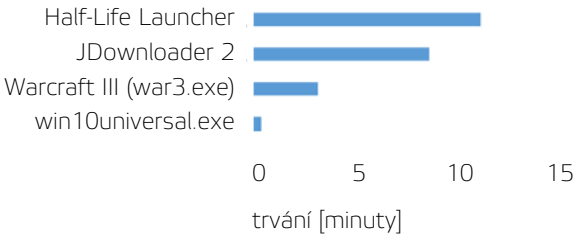
ANALÝZA CHOVÁNÍ V APLIKACÍCH

Porozumění tomu, jaké aplikace zaměstnanci používají, pomáhá společnostem odhalit, kde jsou bezpečnostní rizika, jak jsou využívány drahé licence nebo kde lze zlepšit produktivitu práce.

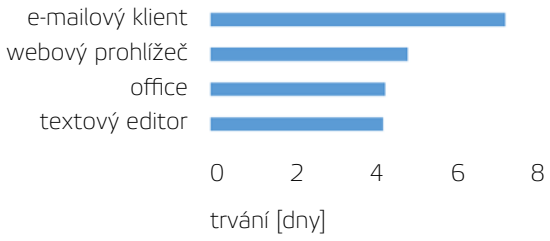
Omezili jste rizikové aplikace, které by mohly být využívány zaměstnanci.

Jasně určená pravidla pro používání aplikací zlepšují zabezpečení společnosti.

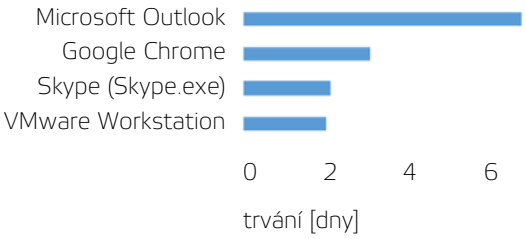
Jaké jsou nejčastější rizikové skupiny?



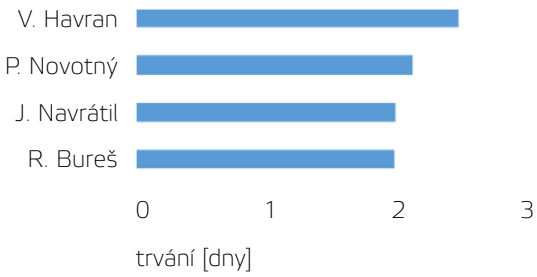
Jak zaměstnanci využívali pracovní čas?



Jaké jsou nejčastější aktivity?



Kdo je nejaktivnější?



Doporučení:

- Kontrolujte, jaké aplikace jsou využívány. Zhodnoťte, jestli kategorie aplikací nepotřebují úpravu.
- Nastavte politiky pro aplikace, abyste zamezili využívání rizikových či nebezpečných aplikací.
- Nastavte pravidelné automatizované reporty na využití aplikací.

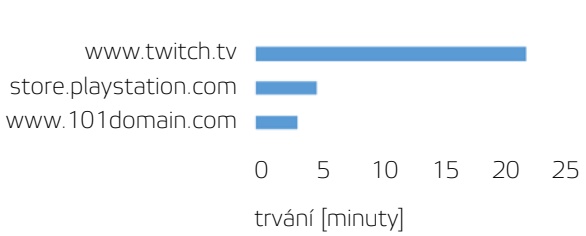
ANALÝZA CHOVÁNÍ NA WEBU

Porozumění tomu, jaké weby zaměstnanci navštěvují, pomáhá společnostem odhalit, kde jsou bezpečnostní rizika nebo kde lze zlepšit produktivitu práce.

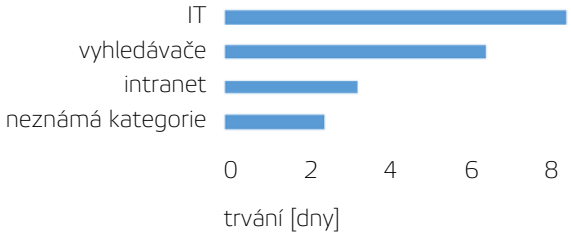
Omezili jste rizikové webové stránky, které by mohli zaměstnanci navštěvovat.

Jasně určená pravidla pro navštěvování webových stránek zvětšují zabezpečení společnosti.

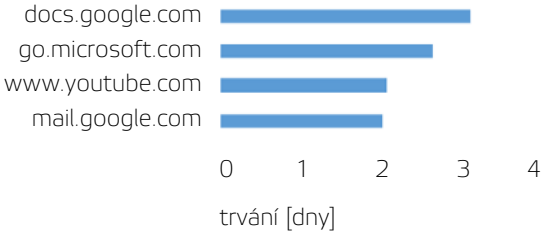
Jaké jsou nejčastější rizikové aktivity?



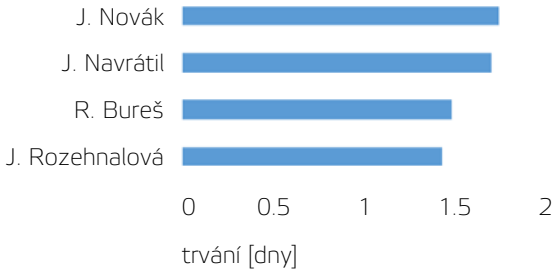
Jak zaměstnanci využívali pracovní čas?



Jaké jsou nejčastější aktivity?



Kdo je nejaktivnější?



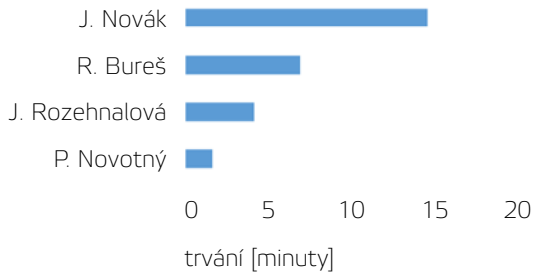
Doporučení:

- Kontrolujte, jaké webové stránky jsou navštěvovány. Zhodnoťte, jestli kategorie webových stránek nepotřebují úpravu.
- Nastavte politiky pro webové stránky, abyste zamezili využívání rizikových či nebezpečných webů.
- Nastavte pravidelné automatizované reporty o navštěvovaných webových stránkách.

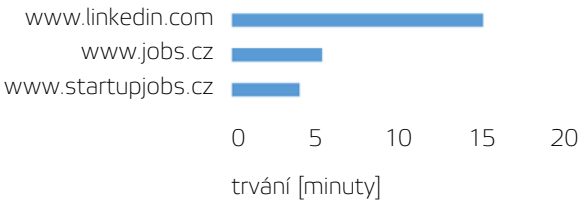
ANALÝZA VYHLEDÁVÁNÍ NOVÉHO ZAMĚSTNÁNÍ NA WEBU

Zaměstnanci, kteří se rozhodnou opustit společnost, představují významné bezpečnostní riziko. Pokud nastoupí do nového zaměstnání, například ke konkurenci, a vezmou si s sebou důležité dokumenty, tak škody pro společnost mohou být značné.

Kdo je nejaktivnější?



Co byly nejčastější činnosti?



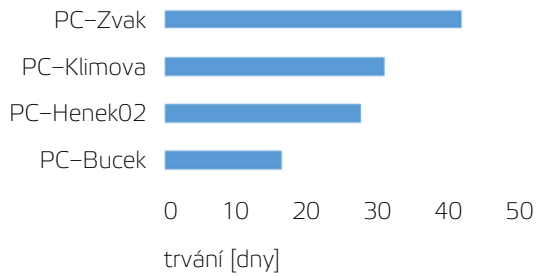
Doporučení:

- Pravidelně kategorizujte monitorované webové stránky k vyhledávání nového zaměstnání.
- Nastavte e-mailová varování, když někdo navštěvuje webové stránky k vyhledávání nového zaměstnání ve velké míře.

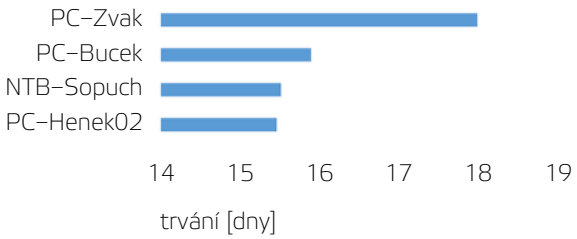
VYUŽITÍ IT ZDROJŮ – POČÍTAČE

Efektivita využití počítačů společnosti je důležitá pro porozumění toho, kde lze uspořit prostředky.

Doba běhů počítačů



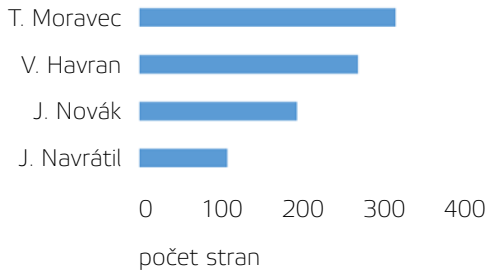
Které počítače byly nejvíce nečinné?



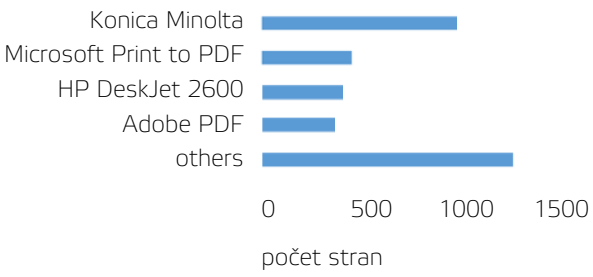
VYUŽITÍ IT ZDROJŮ – TISK

Přehled o využití tisku vám pomůže pochopit, jestli tisknuté dokumenty představují pro společnost bezpečnostní riziko nebo zbytečně vynaložené náklady.

Tisknoucí uživatelé



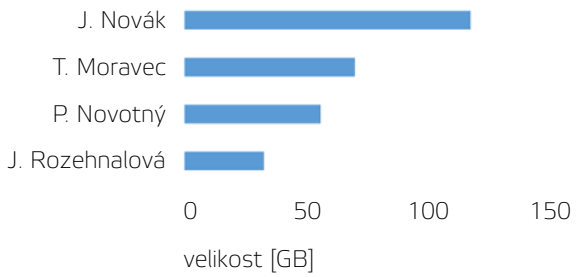
Tiskárny



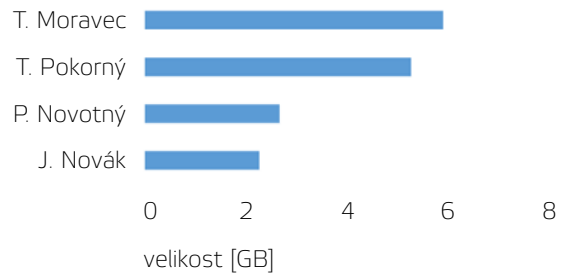
VYUŽITÍ IT ZDROJŮ – SÍŤOVÝ PROVOZ

Velké zatížení sítě nadměrným stahováním či odesíláním dat může pro společnost indikovat bezpečnostní riziko nebo snížení produktivity práce ostatních zaměstnanců.

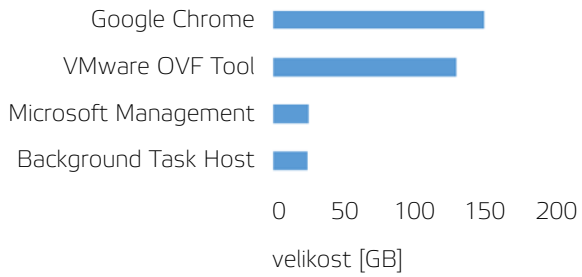
Uživatelé stahující data



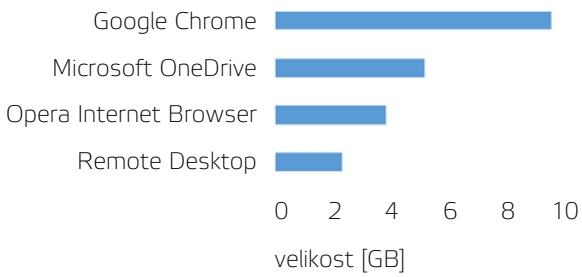
Uživatelé odesílající data



Aplikace stahující data



Aplikace odesílající data



O SAFETICA TECHNOLOGIES

Jsme Safetica Technologies, česká softwarová společnost. Přinášíme řešení na ochranu dat, které je dostupné pro malé a střední podniky. V Safetica totiž věříme, že si každá firma zaslouží, aby její citlivá data zůstala v bezpečí.

170 000+ chráněných zařízení

1 400+ spokojených zákazníků

95+ zemí

70+ expertů

TECHNOLOGICKÉ ALIANCE

ESET ENJOY SAFER TECHNOLOGY™

Microsoft

FORTINET Fabric-Ready

OCENĚNÍ A ÚSPĚCHY

Gartner

RED HERRING WINNER 100 EUROPE

SC MAGAZINE AWARDS WINNER Honored in the U.S.

CYBER SECURITY EXCELLENCE AWARDS WINNER 2019

Info Security Products Guide 2019 GLOBAL EXCELLENCE BRONZE

A co vaše data?

Vyzkoušejte online demo!

safetica®